

CONSOLE ADMIN > DEPLOY CLIENT APPS

Désactiver les gestionnaires de mots de passe du navigateur à l'aide de la gestion de l'appareil

Afficher dans le centre d'aide:

<https://bitwarden.com/help/deactivate-browser-password-managers/>

Désactiver les gestionnaires de mots de passe du navigateur à l'aide de la gestion de l'appareil

Cet article vous guidera sur comment désactiver divers gestionnaires de mots de passe intégrés au navigateur web en utilisant les politiques de sécurité de groupe. Ces étapes aideront à prévenir que les identifiants d'entreprise soient enregistrés et synchronisés avec des comptes personnels. Vous pouvez également envisager de déployer [l'extension de navigateur Bitwarden sur tous les navigateurs](#) dans le cadre de cette même politique.

Désactiver avec Windows GPO

⇒ Désactiver Edge

1. Ouvrez l'éditeur de gestion des politiques de sécurité de groupe sur votre serveur Windows que vous gérez.
2. Téléchargez le modèle de stratégie Edge approprié .
3. Dans l'Éditeur de politiques de sécurité de groupe, créez une nouvelle GPO pour Edge et donnez-lui un nom approprié.
4. Choisissez votre portée désirée.
5. Cliquez avec le bouton droit sur le nouvel **Objet** de la Politique de Sécurité de Groupe → **Éditer**.
6. Dans l'Éditeur de gestion des politiques de groupe, allez à **Configuration de l'utilisateur** → **Politiques de sécurité** → **Modèles administratifs** → **Microsoft Edge**.
7. Définissez les politiques de sécurité suivantes :
 - Ouvrez "Gestionnaire de mots de passe et protection", désactivez la politique **Permettre l'enregistrement des mots de passe dans le gestionnaire de mots de passe**.
 - Désactivez la politique **Activer le remplissage automatique pour les adresses**.
 - Désactivez la politique **Activer le remplissage automatique pour les instruments de paiement**.
 - Optionnellement, vous pouvez activer la politique **Désactiver la synchronisation des données en utilisant les services de synchronisation de Microsoft**.

Une fois terminé, les **paramètres** de la GPO devraient afficher ce qui suit :

User Configuration (Enabled)		
Policies		
Administrative Templates		
Policy definitions (ADMX files) retrieved from the local computer.		
Microsoft Edge		
Policy	Setting	Comment
Disable synchronization of data using Microsoft sync services	Enabled	
Enable AutoFill for addresses	Disabled	
Enable AutoFill for payment instruments	Disabled	
Microsoft Edge/ Password manager and protection		
Policy	Setting	Comment
Enable saving passwords to the password manager	Disabled	

Paramètres Edge

8. Assurez-vous que le lien GPO est activé.

⇒ Désactiver Chrome

1. Ouvrez l'éditeur de gestion des politiques de sécurité de groupe sur votre serveur Windows que vous gérez.

2. Téléchargez les modèles administratifs de Google Chrome.

3. Dans le fichier **ADMX**, copiez ce qui suit:

`policy_templates\windows\adm\chrome.admx`

et

`policy_templates\windows\adm\google.admx`

À `C:\Windows\PolicyDefinitions`

4. Dans le fichier **ADML**, copiez ce qui suit:

`policy_templates\windows\adm\fr-fr\chrome.adml`

et

`policy_templates\windows\adm\fr-fr\google.adml`

À `C:\Windows\PolicyDefinitions\fr-fr`

5. Dans l'Éditeur de politiques de sécurité de groupe, créez une nouvelle GPO pour Chrome et donnez-lui un nom approprié.

6. Choisissez votre portée désirée.

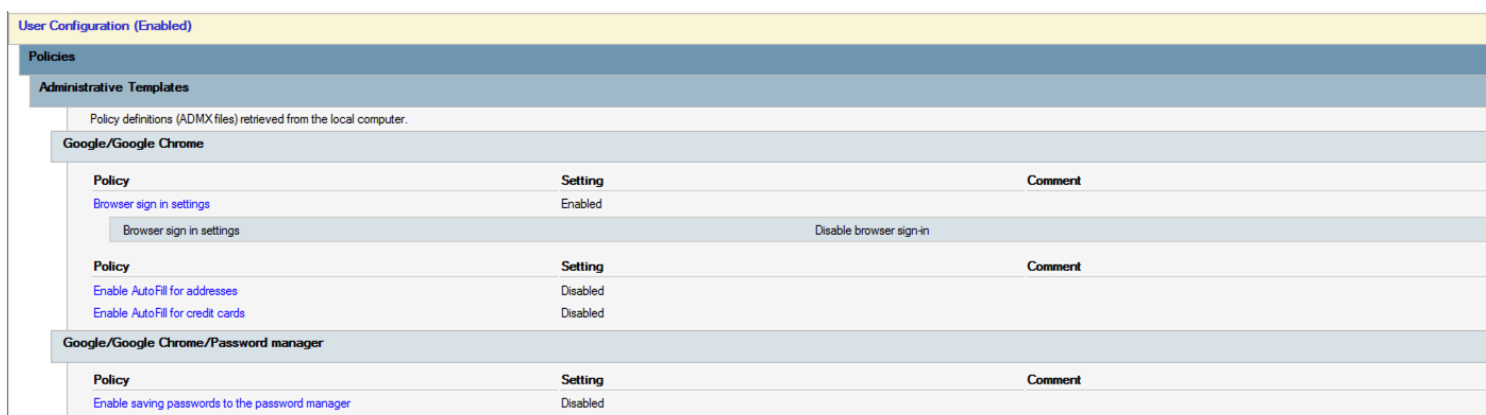
7. Cliquez avec le bouton droit sur l'**Objet de Politique de Groupe** → **Éditer**.

8. Allez à **Configuration de l'utilisateur** → **Politiques de sécurité** → **Modèles administratifs** → **Google** → **Google Chrome**.

9. Éditez les paramètres suivants :

- Sous "Gestionnaire de mots de passe", désactivez la politique **Permettre l'enregistrement des mots de passe dans le gestionnaire de mots de passe**.
- Désactivez la politique **Activer le remplissage automatique pour les adresses**.
- Désactivez la stratégie **Activer la saisie automatique pour les cartes de crédit**.

10. Une fois terminé, les **paramètres** du GPO devraient afficher ce qui suit :



The screenshot shows the Group Policy Editor interface. At the top, it says "User Configuration (Enabled)". Under "Policies", there is a section for "Administrative Templates". Below that, it says "Policy definitions (ADMX files) retrieved from the local computer." The main section is titled "Google/Google Chrome" and contains a table of policies. The table has three columns: "Policy", "Setting", and "Comment".

Policy	Setting	Comment
Browser sign in settings	Enabled	
Browser sign in settings	Disabled	Disable browser sign-in
Enable AutoFill for addresses	Disabled	
Enable AutoFill for credit cards	Disabled	

Below this, there is another section titled "Google/Google Chrome/Password manager" with a table of policies:

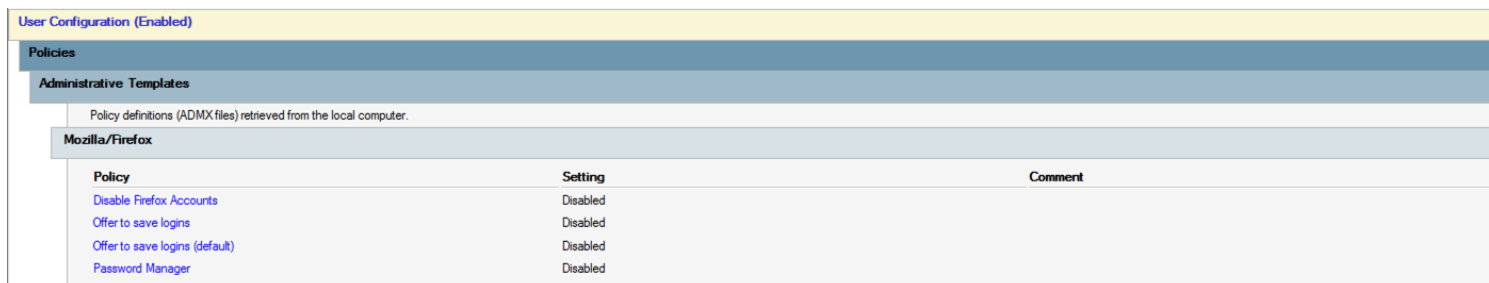
Policy	Setting	Comment
Enable saving passwords to the password manager	Disabled	

Chrome Settings

11. Assurez-vous que le lien GPO est activé.

⇒ Désactiver Firefox

- Ouvrez l'Éditeur de politiques de sécurité de groupe sur votre serveur Windows que vous gérez.
- Téléchargez le dernier fichier .zip des modèles de politiques de sécurité Firefox.
- Copier le fichier **ADMX** :
DE le dossier téléchargé `policy_templates_v1.##\windows\firefox.admx & mozilla.admx`
À `C:\Windows\PolicyDefinitions`
- Copier le fichier **ADML**
DE `policy_templates\windows\fr-fr\firefox.adml & mozilla.adml`
À `C:\Windows \PolicyDefinitions\fr-fr`
- Dans l'Éditeur de Politiques de Sécurité de Groupe, créez une nouvelle GPO pour FireFox et donnez-lui un nom approprié.
- Choisissez votre portée désirée.
- Cliquez avec le bouton droit sur la **nouvelle politique de sécurité de groupe** → **Éditer**.
- Ouvrez **Configuration de l'utilisateur** → **Politiques de sécurité** → **Modèles administratifs** → **Mozilla** → **Firefox**.
- Localisez et éditez les politiques de sécurité suivantes :
 - Désactivez la politique **Désactiver les comptes Firefox**.
 - Désactivez la politique **Proposer d'enregistrer les identifiants**.
 - Désactivez la politique **Offrir pour enregistrer les identifiants (par défaut)**.
 - Désactivez la politique de sécurité **Gestionnaire de mots de passe**.
- Une fois terminé, les **paramètres** de la GPO devraient afficher ce qui suit :



The screenshot shows the Group Policy Editor interface. At the top, it says 'User Configuration (Enabled)'. Below that, there are sections for 'Policies', 'Administrative Templates', and 'Mozilla/Firefox'. Under 'Mozilla/Firefox', there is a table with the following data:

Policy	Setting	Comment
Disable Firefox Accounts	Disabled	
Offer to save logins	Disabled	
Offer to save logins (default)	Disabled	
Password Manager	Disabled	

Firefox Settings

11. Assurez-vous que le lien GPO est activé.

Comment vérifier si cela a fonctionné ?

Vérifiez que les étapes précédentes ont fonctionné correctement pour votre configuration :

⇒Edge

1. On a user's computer, Open the command line, and run:
`gpupdate /force.`
2. Open Edge, then click the three dots for settings ... → **Settings** → **Passwords**.
3. Ensure "Offer to save passwords" is turned off and managed by the organization.

📘 Note

Sign-in automatically is still checked because there is no policy setting to turn this off.

Any logins previously saved in Edge will not be removed and will continue to be displayed to the user, despite autofill being disabled. Be sure to instruct the user to [import any saved logins](#) into Bitwarden before deleting them from Edge.

⇒Chrome

1. On a user's computer, Open the command line, and run:
`gpupdate /force.`
2. Open Chrome and click the **profile icon** on the top right. See that the user is not signed in.
3. Open Chrome, then click the three dots ... → **Settings** → **Passwords**. See that **Offer to save passwords** is unchecked and managed by the organization.

⇒Firefox

1. On a user's computer, Open the command line, and run:
`gpupdate /force.`
2. Open Firefox and select **Logins and Passwords** from the menu bar.
3. Ensure that a "Blocked Page" message is displayed.

Désactiver sur Linux

⇒Chrome

To disable the Chrome Password Manager via group policy:

1. Download the [Google Chrome .deb or .rpm](#) for Linux.
2. Download the [Chrome Enterprise Bundle](#).
3. Unzip the Enterprise Bundle ([GoogleChromeEnterpriseBundle64.zip](#) or [GoogleChromeEnterpriseBundle32.zip](#)) and open the `/Configuration` folder.
4. Make a copy of the `master_preferences.json` (in Chrome 91+, `initial_preferences.json`) and rename it `managed_preferences.json`.
5. To [disable](#) Chrome's built-in password manager, add the following to `managed_preferences.json` inside of `"policies": { }`:

Plain Text

```
{  
  "PasswordManagerEnabled": false  
}
```

6. Create the following directories if they do not already exist:

Plain Text

```
mkdir /etc/opt/chrome/policies  
mkdir /etc/opt/chrome/policies/managed
```

7. Move `managed_preferences.json` into `/etc/opt/chrome/policies/managed`.

8. As you will need to deploy these files to users' machines, we recommend making sure only admins can write files in the `/managed` directory.

Plain Text

```
chmod -R 755 /etc/opt/chrome/policies
```

9. Additionally, we recommend admins should add the following to files to prevent modifications to the files themselves:

Plain Text

```
chmod 644 /etc/opt/chrome/policies/managed/managed_preferences.json
```

10. Using your preferred software distribution or MDM tool, deploy the following to users' machines:

1. Google Chrome Browser
2. `/etc/opt/chrome/policies/managed/managed_preferences.json`

Note

For more help, refer to Google's [Chrome Browser Quick Start for Linux](#) guide.

⇒ Firefox

To disable the Firefox Manager via group policy:

1. Download [Firefox for Linux](#).

2. Open a terminal and navigate to the directory your download has been saved to. For example:

```
cd ~/Downloads
```

3. Extract to contents of the downloaded file:

Plain Text

```
tar xjf firefox-*.tar.bz2
```

The following commands must be executed as root, or preceded by `sudo`.

4. Move the uncompressed Firefox folder to `/opt`:

Plain Text

```
mv firefox /opt
```

5. Create a symlink to the Firefox executable:

Plain Text

```
ln -s /opt/firefox /usr/local/bin/firefox
```

6. Download a copy of the desktop file:

Plain Text

```
wget https://raw.githubusercontent.com/mozilla/sumo-kb/main/install-firefox-linux/firefox.desktop -P /usr/local/share/applications
```

7. To disable Firefox's built-in password manager, add the following to `policies.json` inside of `"policies": {}`:

Plain Text

```
{  
  "PasswordManagerEnabled": false  
}
```

8. Create the following directory if it does not already exist:

Plain Text

```
mkdir /opt/firefox/distribution
```

9. Modify the directory with the following:

Plain Text

```
chmod 755 /opt/firefox/distribution
```

10. Additionally, we recommend admins should add the following to files to prevent modifications to the files themselves:

Plain Text

```
chmod 644 /opt/firefox/distribution/policies.json
```

11. Using your preferred software distribution or MDM tool, deploy the following to users' machines:

12. Firefox Browser

13. `/distribution/policies.json`

Note

For more help, refer to Firefox's [policies.json Overview](#) or [Policies README](#) on Github.

Désactiver sur MacOS

⇒ Chrome

1. Download the [Google Chrome .dmg](#) or [.pkg](#) for macOS.
2. Download the [Chrome Enterprise Bundle](#).
3. Unzip the Enterprise Bundle ([GoogleChromeEnterpriseBundle64.zip](#) or [GoogleChromeEnterpriseBundle32.zip](#)).
4. Open the `/Configuration/com.Google.Chrome.plist` file with any text editor.
5. To [disable](#) Chrome's built-in password manager, add the following to `com.Google.Chrome.plist`:

Plain Text

```
<key>PasswordManagerEnabled</key>  
<false />
```

6. Convert the `com.Google.Chrome.plist` file to a configuration profile using a conversion tool of your choice.

7. Deploy the Chrome `.dmg` or `.pkg` and the configuration profile using your software distribution or MDM tool to all managed computers.

Note

For more help, refer to Google's [Chrome Browser Quick Start for Mac](#) guide.

For additional information, see [Chrome's documentation](#) for setting up Chrome browser on Mac.

⇒Firefox

1. Download and install [Firefox for Enterprise](#) for macOS.
2. Create a `distribution` directory in `Firefox.app/Contents/Resources/`.
3. In the created `/distribution` directory, create a new file `org.mozilla.firefox.plist`.

Tip

Utilisez le [modèle .plist de Firefox](#) et le [README des politiques de sécurité](#) comme référence.

4. To [disable](#) Firefox's built-in password manager, add the following to `org.mozilla.firefox.plist`:

Plain Text

```
<dict>
  <key>PasswordManagerEnabled</key>
  <false/>
</dict>
```

5. Convert the `org.mozilla.firefox.plist` file to a configuration profile using a conversion tool of your choice.
6. Deploy the Firefox `.dmg` and the configuration profile using your software distribution or MDM tool to all managed computers.

For additional information, see [Firefox's documentation](#) for MacOS configuration profiles.

⇒Edge

1. Download the [Microsoft Edge for macOS .pkg](#) file.
2. In Terminal, use the following command to create a `.plist` file for Microsoft Edge:

Plain Text

```
/usr/bin/defaults write ~/Desktop/com.microsoft.Edge.plist RestoreOnStartup -int 1
```

3. Use the following command to convert the `.plist` from binary to plain text:

Plain Text

```
/usr/bin/plutil -convert xml1 ~/Desktop/com.microsoft.Edge.plist
```

4. To **disable** Edge's built-in password manager, add the following to **com.microsoft.Edge.plist**:

Plain Text

```
<key>PasswordManagerEnabled</key>  
<false/>
```

5. Deploy the Edge **.pkg** and the configuration profile using your software distribution or MDM tool to all managed computers.

 **Tip**

Pour obtenir une aide spécifique à Jamf, reportez-vous à la documentation de Microsoft sur [la configuration des paramètres de stratégie Microsoft Edge sur macOS avec Jamf](#).

For additional information, see [Edge's documentation](#) for configuration profiles.